7/13/04 DFW AF/3621/#

DOCKET NO.: MSFT-0135/147325.1

PATENT

O I P E JC151
JUL 1 2 2004
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:
Marcus Peinado et al.

Confirmation No.: 9494

Application No.: 09/525,510

Group Art Unit: 3621

Filing Date: March 15, 2000

Examiner: Backer, Firmin

For: Releasing Decrypted Digital Content To An Authenticated Path

EXPRESS MAIL LABEL NO: EV 386720708 US
DATE OF DEPOSIT: July 12, 2004

EV386720708US

MS Appeal Brief - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF TRANSMITTAL PURSUANT TO 37 CFR § 1.192

Transmitted herewith in triplicate is the APPEAL BRIEF in this application with respect to the Notice of Appeal received by The United States Patent and Trademark Office on **May 10, 2004**.

□ Applicant(s) has previously claimed small entity status under 37 CFR § 1.27 .

□ Applicant(s) by its/their undersigned attorney, claims small entity status under 37 CFR § 1.27 as:

□ an Independent Inventor

□ a Small Business Concern

□ a Nonprofit Organization.

□ Petition is hereby made under 37 CFR § 1.136(a) (fees: 37 CFR § 1.17(a)(1)-(4) to extend the time for response to the Office Action of to and through comprising an extension of the shortened statutory period of month(s).

	SMALL ENTITY		NOT SMALL ENTITY	
	RATE	FEE	RATE	FEE
☒ APPEAL BRIEF FEE	$165	$	$330	$330.00
□ ONE MONTH EXTENSION OF TIME	$55	$	$110	$
□ TWO MONTH EXTENSION OF TIME	$210	$	$420	$
□ THREE MONTH EXTENSION OF TIME	$475	$	$950	$
□ FOUR MONTH EXTENSION OF TIME	$740	$	$1480	$
□ FIVE MONTH EXTENSION OF TIME	$1005	$	$2010	$
□ LESS ANY EXTENSION FEE ALREADY PAID	minus	($)	minus	($)
TOTAL FEE DUE		$0		$330.00

☒ The Commissioner is hereby requested to grant an extension of time for the appropriate length of time, should one be necessary, in connection with this filing or any future filing submitted to the U.S. Patent and Trademark Office in the above-identified application during the pendency of this application. The Commissioner is further authorized to charge any fees related to any such extension of time to Deposit Account 23-3050. This sheet is provided in duplicate.

☒ A check in the amount of **$330.00** is attached. Please charge any deficiency or credit any overpayment to Deposit Account No. 23-3050.

□ Please charge Deposit Account No. 23-3050 in the amount of **$ .00**. This sheet is attached in duplicate.

☒ The Commissioner is hereby requested to grant an extension of time for the appropriate length of time, should one be necessary, in connection with this filing or any future filing submitted to the U.S. Patent and Trademark Office in the above-identified application during the pendency of this application. The Commissioner is further authorized to charge any fees related to any such extension of time to deposit account 23-3050. This sheet is provided in duplicate.

Date: July 12, 2004

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439

© 2004 WW

DOCKET NO.: MSFT-0135 / 147325.1

PATENT

OIPE JC151
JUL 1 2 2004
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:

Marcus Peinado et al.

Serial No.: 09/525,510

Filed: March 15, 2000

For: Releasing Decrypted Digital Content to an Authenticated Path

Group Art Unit: 3621

Examiner: Firmin Backer

APPELLANTS' BRIEF FILED UNDER 37 C.F.R. §1.192

APPELLANTS' BRIEF

Pursuant to the Notice of Appeal mailed on May 10, 2004, set forth below is Appellants' Brief. Two additional copies of this Brief are enclosed.

REAL PARTY IN INTEREST

The real party in interest is Microsoft Corporation by virtue of an Assignment from Marcus Peinado, Paul England, and Frank Yerrace (Appellants) recorded on October 17, 2000 at Reel 011193, Frame 0127.

07/15/2004 HALI11 00000030 09525510
01 FC:1402 330.00 OP

RELATED APPEALS AND INTERFERENCES

No related appeals and interferences are known by Appellants.

STATUS OF CLAIMS

Claims 1-46 are pending in the present application, as filed and unamended. All of the claims were finally rejected under 35 U.S.C. § 103(a) in an Office Action mailed November 13, 2003. All claims are at issue in this Appeal. A copy of the claims involved in this Appeal is contained in an Appendix I attached hereto.

STATUS OF AMENDMENTS

The claims of the present application have not been amended. At present, then, claims 1-46 remain pending in the present application, with claims 1 and 24 being independent. As set forth in the final Office Action mailed November 13, 2003, all claims stand finally rejected. No new amendments to the claims are proposed by Appellants.

SUMMARY OF THE INVENTION

Digital rights management and enforcement is highly desirable in connection with digital content such as digital audio, digital video, digital text, digital data, digital multimedia, etc., where such digital content is to be distributed to users. Upon being received by the user, such user renders or 'plays' the digital content with the aid of an appropriate rendering device such as a media player on a personal computer or the like.

Typically, a content owner or rights-owner, such as an author, a publisher, a broadcaster, etc. (hereinafter "content owner"), wishes to distribute such digital content to a user or recipient in exchange for a license fee or some other consideration. Such content owner, given the choice, would likely wish to restrict what the user can do with such distributed digital content. For example, the content owner would like to restrict the user from copying and re-distributing such content to a second user, at least in a manner that denies the content owner a license fee from such second user.

In addition, the content owner may wish to provide the user with the flexibility to purchase different types of use licenses at different license fees, while at the same time holding the user to the terms of whatever type of license is in fact purchased. For example, the content owner may wish to allow distributed digital content to be played only a limited number of times, only for a certain total time, only on a certain type of machine, only on a certain type of media player, only by a certain type of user, etc. However, after distribution has occurred, such content owner has very little if any actual control over the digital content. (page 2, line 17 – page 3, line 16).

Thus, in connection with the present invention, an enforcement architecture 10 is provided that controls rendering or playing of arbitrary forms of digital content 12, based on a corresponding digital license 16. Such controlled rendering is performed such that the digital content 12 will only be rendered as specified by the content owner in the digital license 16, even though the digital content 12 is to be rendered on a computing device 14 which is not under the control of the content owner.

When a rendering application 34 sends digital content 12 to an ultimate destination 60, it is to be recognized that the digital content 12 'flows' in a path 58 therebetween by way of one or more modules 62 that define such path 58. Such path 58 may include multiple branches, junctions, loops, and the like, and the modules 62 may include software modules and hardware modules including software. For example, for audio-based digital content 12, the modules 62 may include modules performing noise reduction, equalization, balance, and frequency filtering functions, among others. Correspondingly, for multimedia-based digital content 12, the modules 62 may include the aforementioned audio-function modules as well as various video-function modules, synchronization modules, and the like. (page 54, line 13 – page 55, line 6).

In the present invention, then, such path 58 is authenticated to ensure that each constituent module 62 in the path 58 can be trusted by the DRM system 32. Otherwise, the potential exists that one or modules 62 in the path can be employed by a nefarious entity to obtain the digital content 12 in an unencrypted or otherwise malleable form as such digital content 12 traverses such path 58. Assuming the path authentication is successful, the digital content 12 may then be decrypted and forwarded from the rendering application 34 to the ultimate destination 60 by way of such path 58. (page 55, lines 19-26).

To authenticate a path 58, such path is traversed to in effect develop a map of each module in the path 58 and authenticate each path module 62. Such traversal and authentication may be performed by starting at an initial module 62 in the path 58 and authenticating such initial module 62, determining all possible destination modules 62 that receive data from such initial module 62, going to each possible destination module 62 and authenticating each such destination module 62, determining all possible destination modules 62 that receive data from such destination module 62 (step 1507), etc., and iteratively repeating such steps until the map of the path is fully defined and each module 62 has been authenticated. Authenticating each module 62 may be achieved by querying the module 62 for the path and file name of the executable file from which such module 62 arose (i.e., on a hard drive, a server, etc.), and the memory address for the module 62 as it resides in dynamic memory (i.e., RAM or the like). From the executable file, a signature is then located and checked to ensure the executable file was not tampered with, among other things. Also, a certificate associated with the module 62 may be reviewed. In addition, the module 62 as it resides in dynamic memory may be checked to ensure that such module 62 as it resides in dynamic memory does not materially differ from the executable file to ensure that the module 62 as it resides in dynamic memory was not tampered with, among other things. If a module 62 in the path 58 fails to authenticate itself and the corresponding license 16 is silent on the subject, the path 58 is suspect and digital content 12 is not released thereto. (page 57, line 12 – page 58, line 7, page 59, lines 6-17).

Claims 1 and 24 are the independent claims in the present application which are presented in this appeal and are summarized as follows:

Claim 1 recites a method for releasing digital content to a rendering application, where the rendering application forwards the digital content to an ultimate destination by way of a path therebetween. Significantly, the path is defined by at least one module and the digital content is initially in an encrypted form.

In the method, an authentication of at least a portion of the path is performed to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. If in fact each such defining module is to be trusted based on the authentication, the encrypted digital content is decrypted and forwarded to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

Claim 24 recites substantially the same subject matter as claim 1, albeit as a computer-readable medium having computer-executable instructions thereon that perform the method.

Thus, in the present invention, and as recited in the independent claims, encrypted digital content is decrypted and released to a destination by way of a path thereto, where the path is defined by modules that form such path, but only if at least a portion of the path is authenticated to determine that each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. If so, the digital content is decrypted and is forwarded toward such authenticated path.

To summarize, then, the present invention requires –

(1) a rendering application forwarding digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module;

(2) an authentication of the path; and

(3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

The rendering application may be any application that renders content, such as an audio player rendering audio from audio content, a video player rendering video from video content, a visual renderer rendering a picture from picture content, or the like. Significantly, the path is not merely a wire or a communications channel, but is defined by interconnected modules, such as for example audio filters, video filters, picture filters, and the like. Also significantly, inasmuch as the content passing through the modules / filters that define the path is to be decrypted content, such modules / filters of the path must be trusted to handle the decrypted content in a trusted manner, and are therefore each authenticated to determine trustworthiness. Such trust is for example with regard to the fact that the modules / filters defining the path will not copy the decrypted content for nefarious purposes. As may be appreciated, in the course of being authenticated, a particular module may prove its trustworthiness by, for example, proffering a digital certificate issued by an entity that may itself be deemed to be trustworthy. Thus, and again, the present invention is especially useful when the encrypted content is of a type that should not be copied in a decrypted form, such as for example copyright-protected audio and/or video and/or picture content.

ISSUE

Did the Examiner commit error in rejecting claims 1-46 under 35 U.S.C. §103(a) as being obvious over Matsuzaki et al. (U.S. Patent No. 6,058,476) in view of Patel (U.S. Patent No. (6,374,355)?

GROUPING OF CLAIMS

The Examiner has treated together all of the claims pending in the present application. For purposes of the present appeal, Appellants respectfully submit that all of rejected claims 1-46 stand or fall together. Hence, Appellants submit claims 1-46 as a single group for purposes of the present appeal. Appellants also submit that claim 1 be designated as representative of the single group.

ARGUMENT

The Examiner's rejection of claims 1-46 as being obvious over Matsuzaki in view of Patel is improper.

A. The Examiner's Rejection

In the fourth and final Office Action mailed November 13, 2003, the Examiner maintains the rejection of claims 1-46 under 35 U.S.C. § 103(a) as being obvious over Matsuzaki in view of Patel. In particular, and turning to the previous (third) Office Action mailed June 5, 2003 (Paper No. unknown), the Examiner rejected claims 1-46 under section 103(a), stating with regard to claims 1 and 24 essentially that Matsuzaki discloses all features of the claims except authenticating at least a portion of a path between a rendering application and an ultimate destination. Nevertheless, the Examiner continues by asserting that Patel discloses such an authentication, and then concludes by asserting it would be obvious to modify Matsuzaki to include Patel path authentication for the reason that 'this would a [sic] communication path to facilitate communication between the devices' (item 4, pages 2-3).

In the final Office Action itself, the Examiner in maintaining the rejection of claims 1-46 repeats the substance thereof, and also provides a Response to Arguments at pages 10 and 11. In such Response to Arguments points to first and second devices 51, 51 in connection with Fig. 3 of Matsuzaki, and argues that Matsuzaki discloses the first device 51 encrypting data, transmitting same to the second device 52, and such second device 52 decrypting such encrypted data. Presumptively, whatever connection exists between the first and second devices 51, 52 corresponds to the path recited in claims 1-46, except that such a Matsuzaki path clearly contains encrypted data, while the path as recited in claims 1-46 explicitly contains decrypted data. In addition, the Matsuzaki path between the first and second devices 51, 52 is not defined in connection with Fig. 3 or elsewhere, and can only be presumed to be a direct connection such as wired or wireless connection. In contrast, the path of claims 1-46 is specifically recited as being defined by modules that form such path. Since the Matsuzaki path as pointed to by the Examiner is not defined by modules, moreover, such non-existent modules cannot be determined to be trusted to authenticate the Matsuzaki path, as is specifically recited in claims 1-46.

Tellingly, the Response to Arguments does not at all mention Patel.

B. Prior Art

1. Matsuzaki

Matsuzaki discloses a system and method of encrypting content for transmission between a first and a second device such as the first and second devices 51, 52 shown in Fig. 3 thereof. Significantly, in any embodiment of the Matsuzaki reference the first device encrypts the content and then transmits same to the second device in the encrypted form for decryption thereby, presumably by way of some conduit therebetween. As part of the system and method of Matsuzaki, an encryption /

decryption key is developed by and shared with the first and second devices, although the details of such development and sharing are not believed to be especially relevant and therefore are not set forth herein in any detail.

According to the Examiner, one conduit or path between the first and second Matsuzaki devices may be a cable 116 such as that shown in Fig. 9 along with a SCSI controller 121 such as that shown in Fig. 10. Note, though, that all content transmitted by the first device to the second device is encrypted, and that such a Matsuzaki path is not first authenticated before content is released thereto.

Also according to the Examiner, Matsuzaki does disclose decrypting content (cj) at a second encryption IC 56 (Fig. 3) and sending such decrypted content to an MPU 55. However, such decrypted content is not sent by a rendering application to an ultimate destination by way of a path therebetween that is defined by at least one module. Instead, such decrypted content cj is shown and disclosed as being sent directly from the second encryption IC 56 to the MPU 55 without any path-defining intermediate modules therebetween, and as a result, no authentication of such a path is disclosed or suggested nor is decryption and forwarding of the decrypted content cj through the path, but only if the authentication succeeds, disclosed or suggested. Moreover, and at any rate, the decrypted content cj pointed to by the Examiner in Matsuzaki is disclosed as traveling a different route other than the path pointed to by the Examiner in Matsuzaki.

Thus, Matsuzaki does not disclose or suggest decrypted content being transmitted through an authenticated path defined by at least one module inasmuch as Matsuzaki reference need not authenticate any sensitive path such as that between first and second devices 51, 52 of Fig. 3, when the content transmitted along such path is encrypted. Matsuzaki discloses only authenticating a destination or source and sending / receiving encrypted content to / from the authenticated destination or source, and not authenticating a path and sending decrypted content over the authenticated path.

2. Patel

Inasmuch as the Examiner recognizes that Matsuzaki does not authenticate at least a portion of a path, the Examiner cites Patel for as in fact disclosing authenticating at least a portion of a path. Patel discloses a wireless communications system where a mobile unit 20 and a base network 10 (Fig. 2) mutually establish secure over-air communications therebetween by way of exchanging data and then mutually deriving a cryptographic key based on such exchanged data. Such key is then employed to establish encrypted communications channels by which the mobile unit and the base network communicate.

Like Matsuzaki, then, Patel reference does not disclose or suggest decrypting encrypted digital content and forwarding such decrypted content through a path comprising pre-defined modules. Instead, Patel discloses that the path need not be trusted because the content is encrypted while traversing such path. Patel discloses only authenticating a destination or source and sending / receiving encrypted content to / from the authenticated destination or source. Moreover, Patel does not even disclose or suggest that the Patel path is defined by modules through which the Patel data passes. Instead, the Patel path is merely one or more ethereal over-air communications channels.

C. Standard of Review under 35 U.S.C. § 103(a)

It is well established that obviousness under 35 U.S.C. § 103 (and now § 103(a)) is a legal conclusion based upon factual evidence and, therefore, a conclusion of obviousness is reviewed for correctness or error as a matter of law. In re Fine, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir. 1988) (citation omitted).

To reach a proper conclusion under [§ 103(a)], the decision maker must step backward in time and into the shoes worn by [a person having ordinary skill in the art] when the invention was known and just before it was made. In light of all the evidence, the decision maker must then determine whether...the claimed invention as a whole would have been obvious at that time to that person. 35 U.S.C. [§103(a)]. The answer to that question partakes more of the nature of law than of fact, for it is an ultimate conclusion based upon a foundation formed of all the probative facts. In re Fine at 1598, quoting from Panduit Corp. v. Dennison Mfg. Co., 1 U.S.P.Q. 2d 1593, 1595-96 (Fed. Cir. 1987).

It is clear that when making an obviousness rejection under 35 U.S.C. § 103(a), the Examiner has the burden to establish a prima facie case of obviousness. In re Fine, 5 U.S.P.Q. 2d at 1598. When, as in the present case, the Examiner's rejection is based upon a combination of two or more references, the Examiner can satisfy the burden only by showing some objective teaching in the cited references or that knowledge generally available to one of ordinary skill in the art would lead that particular individual to combine the relevant teachings of the references in the manner suggested by the Examiner. In re Fine, 5 U.S.P.Q. 2d at 1598.

Obviousness cannot be established by combining the teachings of the prior art utilizing hindsight reconstruction to pick and choose among isolated disclosures in the prior art and to then reach a conclusion that the claimed invention is in fact obvious. Instead, the Examiner must point to a specific teaching or suggestion, or an incentive, to combine the references in the manner in which they are combined to make the rejection by the Examiner. In re Fine, 5 U.S.P.Q.2d at 1599-1600; See, also, Uniroyal, Inc. v. Rudkin-Wiley Corp., 5 U.S.P.Q.2d 1434, 1438-39 (Fed. Cir. 1988); Carella v. Starlight Archery, 231 U.S.P.Q. 644, 647 (Fed. Cir. 1986); and In re Lalu and Foulletier, 223 U.S.P.Q. 1257, 1258 (Fed. Cir. 1984).

D. Arguments - The Examiner Has Failed to Establish the Required Prima Facie Case of Obviousness Under 35 U.S.C. ' 103(a), and Matsuzaki and Patel Do Not in Fact Disclose or Suggest the Subject Matter Recited

1. Neither Matsuzaki nor Patel discloses (1) a rendering application forwarding digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module; (2) an authentication of the path; and (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

According to the Examiner, Matsuzaki discloses a communications path between first and second devices comprising a cable 116 in Fig. 9 a SCSI controller 121 in Fig. 10. However, Matsuzaki is clear that all communications between the first device and the second device thereof are encrypted. Accordingly, such a Matsuzaki path does not receive decrypted digital content, as is required by claims 1 and 24. Moreover, and as the Examiner concedes, such a path is not authenticated in any manner prior to forwarding any such content therethrough, as is also required by claims 1 and 24.

While Matsuzaki does disclose decrypting content (cj) at a second encryption IC 56 (Fig. 3) and sending such decrypted content to an MPU 55, such decrypted content is not disclosed or suggested as being sent by a rendering application as is required by claims 1 and 24, and is not disclosed or suggested as being forwarded to an ultimate destination by way of a path therebetween, where the path is defined by at least one module, as is also required by claims 1 and 24. Instead, such decrypted content cj is shown and disclosed as being sent directly from the second encryption IC 56 to the MPU 55 without any path-defining intermediate modules therebetween Further, inasmuch as the decrypted content cj is not sent by way of path-defining intermediate modules, no authentication of such a path is disclosed or suggested, as is required by claims 1 and 24, nor is decryption and forwarding of the decrypted content cj through the path, but only if the authentication succeeds, disclosed or suggested, as is required by claims 1 and 24.

At any rate, the decrypted content cj pointed to by the Examiner in Matsuzaki is disclosed as traveling a different route other than the path pointed to by the Examiner in Matsuzaki, and therefore cannot be employed to show that Matsuzaki discloses or suggests decrypted content being transmitted through an authenticated path defined by at least one module, as is required by claims 1 and 24.

The Examiner admits that Matsuzaki fails to disclose or suggest authenticating any portion of the Matsuzaki path between first and second devices. Nevertheless, the Examiner continues by arguing that Patel discloses authenticating at least a portion of a path. However, and again, Patel discloses in connection with a wireless communications system that a mobile unit and a base network mutually establish a communications channels by which the mobile unit and the base network can exchange encrypted data. Like Matsuzaki, then, Patel does not disclose or suggest decrypting encrypted digital content and forwarding such decrypted content through a path comprising pre-defined modules, as is required by claims 1 and 24. As with Matsuzaki reference, Patel instead discloses that the path need not be trusted because the content is encrypted while traversing such path. Thus, and again, whereas claims 1 and 24 require both authenticating a path comprising pre-defined modules and sending decrypted content over the authenticated path, both Patel and Matsuzaki disclose only authenticating a destination or source and sending / receiving encrypted content to / from the authenticated destination or source.

Moreover, Patel does not even disclose or suggest that the Patel path is defined by modules through which the Patel data passes, as is the case with claims 1 and 24. Instead, in Patel, the path is merely one or more ethereal over-air communications channels.

To summarize, then, both Matsuzaki and Patel teach only that first and second devices authenticate each other, and not a path defined by modules therebetween, as is required by claims 1 and 24. Moreover, Matsuzaki and Patel would not teach that either of such first and second devices authenticates such a module-defining path therebetween for the reason that the content traverses non-module-defining paths, and at any rate is encrypted during traversal of a path and therefore cannot be appropriated in a 'naked' form while in the path.

2. The Examiner has failed to cite an objective teaching, suggestion, or disclosure that would support combining the teachings of Matsuzaki and Patel to form a system with (1) a rendering application forwards digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module; (2) an authentication of the path; and (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

In the Final Office Action, the Examiner asserts that although Matsuzaki fails to disclose authenticating at least a portion of a path, Patel in fact teaches such an authentication. However, and as was set forth above, Patel does not in fact teach authenticating any portion of a path defined by modules where the path interconnects a rendering application and an ultimate destination of content sent by such rendering application. In fact, such Patel reference would not teach authenticating any such path inasmuch as (1) the Patel path is an over-air wireless path without any defining modules; (2) such modules by their absence need not be trusted; and (3) the over-air Patel path forwards encrypted data, which by its nature need not be handled by a trusted / authenticated routing. Note that trust in a path is only necessary when the path receives un-encrypted data, which is certainly not the case in Patel, or even in Matsuzaki for that matter.

Again, neither the Matsuzaki reference nor the Patel references disclose (1) an authentication of a path defined by at least one module and (2) a decryption and forwarding of decrypted content through such a path, but only if the authentication succeeds, as is required by claims 1 and 24. Moreover, no object teaching, suggestion, or disclosure exists in either Matsuzaki or Patel that would result in a finding of such elements.

Thus, the Examiner is incorrect in pointing to Patel for the purpose of disclosing or suggesting path authentication such as it is recited in claims 1 and 24 of the present application. As a result, the Examiner has not specifically pointed to anything in any of the cited references that objectively teaches or suggests (1) an authentication of a path defined by at least one module and (2) a decryption and forwarding of decrypted content through such a path, but only if the authentication succeeds, as is required by claims 1 and 24.

3. Matsuzaki and Patel both fail to teach, suggest, or disclose (1) a rendering application forwards digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module; (2) an authentication of the path; and (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

Appellants have thoroughly reviewed the references cited by the Examiner and cannot locate any teaching, suggestion or disclosure of (1) a rendering application that forwards digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module; (2) an authentication of the path; and (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds, all as required by claims 1 and 24. As the Examiner has already conceded, Matsuzaki does not, in fact, disclose such path authentication. Moreover, Patel does not and would not teach such path authentication either, for the reasons set forth above.

Further, both Matsuzaki and Patel actually teach away from the present invention in that both references require encryption of transmitted data over an exposed path. Again, trust in a path is only necessary when the path receives un-encrypted data, which is certainly not the case in Patel or Matsuzaki. In the present invention, such data must be unencrypted for the reason that such data is content traveling from a rendering application such as a media player on a computing device to an ultimate destination such as a speaker of the computing device. As should no doubt be appreciated, if the content were in an encrypted form, such speaker would in effect produce noise and not the rendered content.

Appellants do not contend that the invention is in transmitting data over a path from a source to a destination. Clearly, both Matsuzaki and Patel show such an arrangement. However, Appellants contend that they have invented the presently claimed arrangement including (1) a rendering application that forwards digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module; (2) an authentication of the path; and (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds, all as required by claims 1 and 24. None of the references cited by the Examiner teach the claimed features that sets the present invention apart. Hence, any conclusion that Appellants' claimed invention is obvious would be contrary to the standard of obviousness.

4. The Examiner has failed procedurally to establish a prima facie case of obviousness.

In order to establish a prima facie case of obviousness, the Examiner has the procedural burden of explaining a rejection with a reasonable degree of specificity. Ex parte Blanc, 13 U.S.P.Q. 2d 1383, 1384 (PTO Bd. App. & Int. 1989).

Here the Examiner has concluded that the present invention is obvious in view of a broad rationale obtained from misconstruing the cited references, when in fact neither reference discloses the key features of the present invention, including (1) a rendering application that forwards digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module; (2) an authentication of the path; and (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds. By setting forth such a broad rationale, misconstruing the references, and failing to explain with specificity how one having ordinary skill in the art at the time the invention was made would find the present invention to be obvious, the Examiner has failed, procedurally, to establish a prima facie case of obviousness.

5. Appellants' claimed invention has satisfied a long-felt need.

It is well settled that evidence of long-felt need is directly related to the issue of non-obviousness and must be considered before a conclusion on obviousness is reached. Here, the desire to transmit decrypted content from a rendering application to an ultimate destination by way of a trusted path defined by modules such that the content is not likely to be intercepted while in such path by any of such modules presents a significant problem in designing and developing a digital rights management system.

Specifically, and as should be appreciated, content developers / owners are rightfully loathe to provide digital content that can be intercepted in a 'naked' form and then be widely re-distributed without protection or proper remuneration to such owners. While digital rights management systems have heretofore taken great care, then, to protect such digital content until such content reaches a rendering application, such systems have not likewise taken care to protect the content once rendered by such application and then sent to an ultimate destination by way of a path therebetween. Put simply, such path was a weak link in that the content is in a decrypted form in such path and any defining module therein could therefore be constructed to divert such decrypted content to a location where such diverted content could be copied and re-distributed without protection or proper remuneration to such owners.

In contrast, in the present invention, such path is no longer the weak link inasmuch as each defining module must now be authenticated prior to releasing the decrypted content to such path. Thus, each module in the path and the path itself is authenticated and thus can be trusted not to divert the content therein or otherwise perform any action with regard to the content that would be contrary to the interests of the owners thereof. Accordingly, the present invention has satisfied a long-felt need and, therefore, is not obvious in view of the references cited by the Examiner.

CONCLUSION

Thus, for all of the reasons set forth above, Appellants respectfully submit that the Examiner has failed to show that Matsuzaki and Patel in combination or separately disclose or suggest the invention recited in claims 1 or 24 or any claims depending therefrom. As a result, Appellants respectfully submits that the Examiner has failed to make the required prime facie case that the combination of Matsuzaki and Patel makes obvious such claims or their dependent claims under section 103(a), and that for this reason the section 103(a) rejection should be withdrawn.

In view of the foregoing discussion, it is respectfully submitted that the Examiner's rejection of claims 1-46 is improper and it is respectfully submitted that the rejection of such claims should be reversed by the Board.

Respectfully submitted,

Steven H. Meyer
Registration No. 37,189

Date: July 12, 2004

WOODCOCK WASHBURN LLP
One Liberty Place - 46th Floor
Philadelphia, PA 19103
(215) 568-3100

OIPE JC151
JUL 1 2 2004
PATENT & TRADEMARK OFFICE

APPENDIX I

CLAIMS 1-46

1. (Original) A method for releasing digital content to a rendering application, the rendering application for forwarding the digital content to an ultimate destination by way of a path therebetween, the path being defined by at least one module, the digital content initially being in an encrypted form, the method comprising:

performing an authentication of at least a portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough;

decrypting the encrypted digital content if in fact each such defining module is to be trusted; and

forwarding the decrypted digital content to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

2. (Original) The method of claim 1 wherein the path includes a user mode portion and a kernel portion, the method further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

3. (Original) The method of claim 2 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

4. (Original) The method of claim 2 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

5. (Original) The method of claim 4 comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

6. (Original) The method of claim 1 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

7. (Original) The method of claim 6 further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

8. (Original) The method of claim 7 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

9. (Original) The method of claim 7 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

10. (Original) The method of claim 1 wherein performing the authentication comprises:

traversing the at least a portion of the path to develop a map of each module in the path; and

authenticating each module in the map.

11. (Original) The method of claim 10 wherein performing the authentication further comprises ignoring each module not in the map.

12. (Original) The method of claim 1 wherein performing the authentication comprises:

authenticating an initial module;

determining all first destination modules that receive data from such initial module;

authenticating each such first destination module;

determining all second destination modules that receive data from each such first destination module;

iteratively repeating the authenticating and determining steps for third, fourth, fifth, etc. destination modules until each module in such at least a portion of the path has been determined and authenticated.

13. (Original) The method of claim 12 wherein authenticating the initial module comprises authenticating a module in the at least a portion of the path that is to receive the digital content before any other module in the at least a portion of the path, whereby the initial module leads to fully determining all other modules that define the at least a portion of the path.

14. (Original) The method of claim 12 comprising employing a database device to keep track of all modules determined to be in the at least a portion of the path, whereby already-determined modules in the at least a portion of the path can be recognized.

15. (Original) The method of claim 1 wherein performing an authentication comprises:

for each module in the at least a portion of the path:

receiving from the module a certificate as issued by a certifying authority; and

determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module.

16. (Original) The method of claim 15 wherein performing an authentication further comprises checking a revocation list to ensure that the received certificate has not been revoked.

17. (Original) The method of claim 16 further comprising:

receiving the revocation list from a certifying authority;

storing the received revocation list in a secure location.

18. (Original) The method of claim 15 wherein performing an authentication further comprises refusing to decrypt the encrypted digital content if at least one module in the at least a portion of the path fails to provide an acceptable certificate.

19. (Original) The method of claim 15 wherein performing an authentication further comprises decrypting the encrypted digital content if all the modules in the at least a portion of the path provide an acceptable certificate.

20. (Original) The method of claim 15 wherein performing an authentication further comprises, for each module in the at least a portion of the path that fails to provide an acceptable certificate:

defining a sub-portion of the path including the non-providing module;

scrambling the digital content upon such digital content entering the sub-portion of the path, such scrambled digital content then passing through the modules that define the sub-portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the sub-portion of the path; and

declaring the sub-portion trustworthy.

21. (Original) The method of claim 1 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of the user mode portion of the path and of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

22. (Original) The method of claim 1 wherein the path includes a

tunneled portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the path;

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.

23. (Original) The method of claim 22 wherein the path includes a user mode portion, a kernel portion, and a tunneled portion in the user mode portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the user mode portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the user mode portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the user mode portion of the path.

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the user mode portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.

24. (Original) A computer-readable medium having computer-executable instructions thereon for performing a method for releasing digital content to a rendering application, the rendering application for forwarding the digital content to an ultimate destination by way of a path therebetween, the path being defined by at least one module, the digital content initially being in an encrypted form, the method comprising:

performing an authentication of at least a portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough;

decrypting the encrypted digital content if in fact each such defining module is to be trusted; and

forwarding the decrypted digital content to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

25. (Original) The method of claim 24 wherein the path includes a user mode portion and a kernel portion, the method further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

26. (Original) The method of claim 25 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

27. (Original) The method of claim 25 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

28. (Original) The method of claim 27 comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

29. (Original) The method of claim 24 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

30. (Original) The method of claim 29 further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

31. (Original) The method of claim 30 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

32. (Original) The method of claim 30 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

33. (Original) The method of claim 24 wherein performing the authentication comprises:

traversing the at least a portion of the path to develop a map of each module in the path; and

authenticating each module in the map.

34. (Original) The method of claim 33 wherein performing the authentication further comprises ignoring each module not in the map.

35. (Original) The method of claim 24 wherein performing the authentication comprises:

authenticating an initial module;

determining all first destination modules that receive data from such initial module;

authenticating each such first destination module;

determining all second destination modules that receive data from each such first destination module;

iteratively repeating the authenticating and determining steps for third, fourth, fifth, etc. destination modules until each module in such at least a portion of the path has been determined and authenticated.

36. (Original) The method of claim 35 wherein authenticating the initial module comprises authenticating a module in the at least a portion of the path that is to receive the digital content before any other module in the at least a portion of

the path, whereby the initial module leads to fully determining all other modules that define the at least a portion of the path.

37. (Original) The method of claim 35 comprising employing a database device to keep track of all modules determined to be in the at least a portion of the path, whereby already-determined modules in the at least a portion of the path can be recognized.

38. (Original) The method of claim 24 wherein performing an authentication comprises:

for each module in the at least a portion of the path:

receiving from the module a certificate as issued by a certifying authority; and

determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module.

39. (Original) The method of claim 38 wherein performing an authentication further comprises checking a revocation list to ensure that the received certificate has not been revoked.

40. (Original) The method of claim 39 further comprising:

receiving the revocation list from a certifying authority;

storing the received revocation list in a secure location.

41. (Original) The method of claim 38 wherein performing an authentication further comprises refusing to decrypt the encrypted digital content if at least one module in the at least a portion of the path fails to provide an acceptable

certificate.

42. (Original) The method of claim 38 wherein performing an authentication further comprises decrypting the encrypted digital content if all the modules in the at least a portion of the path provide an acceptable certificate.

43. (Original) The method of claim 38 wherein performing an authentication further comprises, for each module in the at least a portion of the path that fails to provide an acceptable certificate:

defining a sub-portion of the path including the non-providing module;

scrambling the digital content upon such digital content entering the sub-portion of the path, such scrambled digital content then passing through the modules that define the sub-portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the sub-portion of the path; and

declaring the sub-portion trustworthy.

44. (Original) The method of claim 24 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of the user mode portion of the path and of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

45. (Original) The method of claim 24 wherein the path includes a tunneled portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the path;

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.

46. (Original) The method of claim 45 wherein the path includes a user mode portion, a kernel portion, and a tunneled portion in the user mode portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the user mode portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the user mode portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the user mode portion of the path.

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the user mode portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.